ATTACHMENT B
ITEMS TO BE SEIZED AND SEARCHED

Section I

This warrant authorizes the search and seizure of the devices identified in Attachment A (DEVICES) for the following information:

1. Evidence of who used, owned, or controlled the DEVICES, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

2. Any input/output peripheral devices, passwords, data security devices, and related security documentation that could be related to the DEVICES;

3. Evidence of software that would allow someone or something other than the user to control the DEVICES, such as viruses, Trojan horses, spyware, malware, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

4. Evidence of the lack of such malicious software on the DEVICES;

5. Evidence of software designed to protect the DEVICES from other persons, software, devices, or intrusions that may attempt to infiltrate, access, or control the DEVICES, such as pop-up blockers, security software, password protection, and encryption;

6. Evidence of other storage devices being attached to the DEVICES;

7. Evidence of counter-forensic programs and hard drive/computer cleaning programs (and associated data) that are designed to eliminate data from the DEVICES or frustrate the efforts of law enforcement to locate evidence on the DEVICES;

8. Evidence of the times the DEVICES were used;

9. Evidence indicating how and when the DEVICES were accessed or used to determine the chronological context of the DEVICES access, use, and events relating to crimes under investigation and to the DEVICES' users;

10. Evidence of where the DEVICES were used, including evidence of wireless Internet networks and Internet Protocol addresses;

11. Passwords, encryption keys, and other access devices or programs that may be necessary to access the DEVICES;

12. Correspondence and contact information pertaining to counterfeit sports memorabilia or other counterfeit items;

13. Evidence indicating the DEVICES' user's state of mind as it relates to the crimes under investigation;

14. Documentation and manuals that may be necessary to access the DEVICES or to conduct a forensic examination of the DEVICES;

15. Records of or information about Internet Protocol addresses used by the DEVICES;

16. Records of or information about the DEVICES' Internet activity: firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search

terms that the user entered into any Internet search engine, and records of user-typed web addresses;

17. All records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider, as well as any and all records relating to the ownership or use of the DEVICES found; and

18. Documents and records regarding the ownership and/or possession of the searched premises or DEVICES.

Section II

The information identified in Section I shall be searched and seized to locate property, evidence, fruits, and instrumentalities of violations of 18 U.S.C. §1341 (frauds and swindles) and 18 U.S.C. §1343 (fraud by wire, radio, or television).